

TOP STORIES FROM CYBER AND TECH LEADERS

cyberfest magazine

AUTUMN 2026

PREPARING FOR A POST-QUANTUM FUTURE
AI'S IMPACT ON BUSINESS, EDUCATION AND MORE
MEET YOUR SPEAKERS

Entertainment from
Asteria's Playground


cyberfest
2026



FORTEM
INFORMATION TECHNOLOGY

IN COLLABORATION WITH



CYNAM

OPTIMISE

Maximise value.

COMPLIMENTARY

Cloud Insights Health Check

Reduce licensing waste and cloud overspend with a practical review that turns usage data into clear commercial actions.

MAKE EVERY MICROSOFT INVESTMENT WORK HARDER

Fortem reviews your Azure and Microsoft 365 environment and turns complex usage data into clear, prioritised next steps.

- ✓ **LOWER COST AND REMOVE INEFFICIENCY**
Identify Azure waste and underused licences.
- ✓ **IMPROVE RETURN ON INVESTMENT**
Prioritise measurable optimisation actions.
- ✓ **PREPARE FOR COPILOT**
Assess readiness, candidate users and value.

15-35%

AVERAGE POTENTIAL SAVINGS RATE
identified by Cloud Insights

BOOK YOUR COMPLIMENTARY HEALTH CHECK

Scan the QR code to register your interest, or contact Fortem:

hello@fortem-it.com

fortem-it.com | 020 3964 2763



WELCOME TO CYBERFEST 2026

With GCHQ, the National Cyber Security Centre and an incredible ecosystem of defence, education, government, enterprise, researchers and start-ups, much of the work in Cheltenham shapes how the rest of the country stays safe.

Add the emerging technology coming out of the wider Gloucestershire and South West region in robotics, AI and quantum, and you have a concentration of expertise that most cities would envy.

CyNam have been critical to building and shaping this community over the last ten years, so we at Fortem IT teamed up with them to deliver CyberFest 2026.

Cyber security, tech and AI have plenty of dedicated conferences in London and beyond. CyberFest is purposefully smaller in scale, built around the most pressing conversations right now, by the people shaping the outcome. Expect topics that challenge you: the mental health impact of a cyber attack, shadow AI nobody in your business approved and the quantum deadline that keeps getting ignored. Plus panels that highlight mission-driven initiatives and big names such as Jamie Bartlett, the Producer of The Missing Cryptoqueen.

CyberFest is also a space to enjoy yourself. There is a circus at 17:15 (page 20), networking cider tours throughout the day (page 24) and a dedicated Chill Out Space when you need one. Plus plenty of room to sit down and connect with someone new. Great work comes from relationships, and those are often built through conversation and laughter.

In the coming pages, learn more about those behind CyberFest 2026.

Lee Dzendrowski

Solutions Director, Fortem IT

CONTENTS

- 04** Agenda
- 05** Floorplan
- 06** Leading the Future of Secure Technology
- 10** Meet Your Hosts
- 11** Speakers
- 20** Asteria's Playground
- 24** Cyber Resilience: The Necessity of Proof Over Promises
- 28** Networking Cider Tasting Tours
- 29** Prize Draw
- 30** Preparing for a Post-Quantum Future: The Countdown is On
- 32** Cyber Resilience Starts With What You Don't Know You Have
- 34** Auvik Launches AI Agents for IT Operations Grounded in Real-Time Network Data
- 36** The Translation Gap: Why Brilliant Technical Companies Struggle to Convert
- 40** Protect. Manage. Automate. IT for the AI Era
- 42** Key Takeaways from Arctic Wolf's 2026 Threat Report
- 45** 2026 Work Trend Index Annual Report
- 52** You Can't Defend What You Can't See



IN COLLABORATION WITH  CYNAM

CYBERFEST 2026 - AGENDA

10:00 REGISTRATION AND NETWORKING BREAKFAST

10:25 - HOST WELCOME

10:30 - Fortem x CyNam Partnership and the Future of CyberFest

10:45 - How Agentic AI is Disrupting the Cyber Landscape

11:15 - Visibility is the Foundation of Cyber Security

11:40 - Build Resilience Without Overwhelming Smaller Suppliers

12:00 REFRESHMENTS AND NETWORKING BREAK

12:20 - PANEL: Mission Driven and Not-for-Profit Spotlight

12:45 - The Current State of Ransomware

13:10 LUNCH BREAK - LA BOULANGERIE ARTISAN LUNCH PROVIDED

14:00 - PANEL: Cyber Beyond the Cyber Team: Full Business Buy In

14:30 - You Can't Defend What You Can't See: Blind Spots by Design

15:00 - Preparing for a Post-Quantum Future: The Countdown is On

15:20 REFRESHMENTS AND NETWORKING BREAK

15:40 - Stronger Together: Successful Public Sector Technology Partnerships

16:00 - Impact of AI on Education: Exams, Memory and Teachers

16:15 - Nobody Approved This: The Rise of Shadow AI in your Supply Chain

16:35 - PANEL: The Secret Ingredient in Robotics

17:00 - Blame Game: The Mental Health Impact of a Cyber Attack on your Team

17:15 - 17:45 CIRCUS ENTERTAINMENT BY ASTERIA'S PLAYGROUND

17:45 FOOD BREAK - DUNKERTONS VOUCHERS PROVIDED

18:45 - HOST WELCOME TO EVENING AGENDA

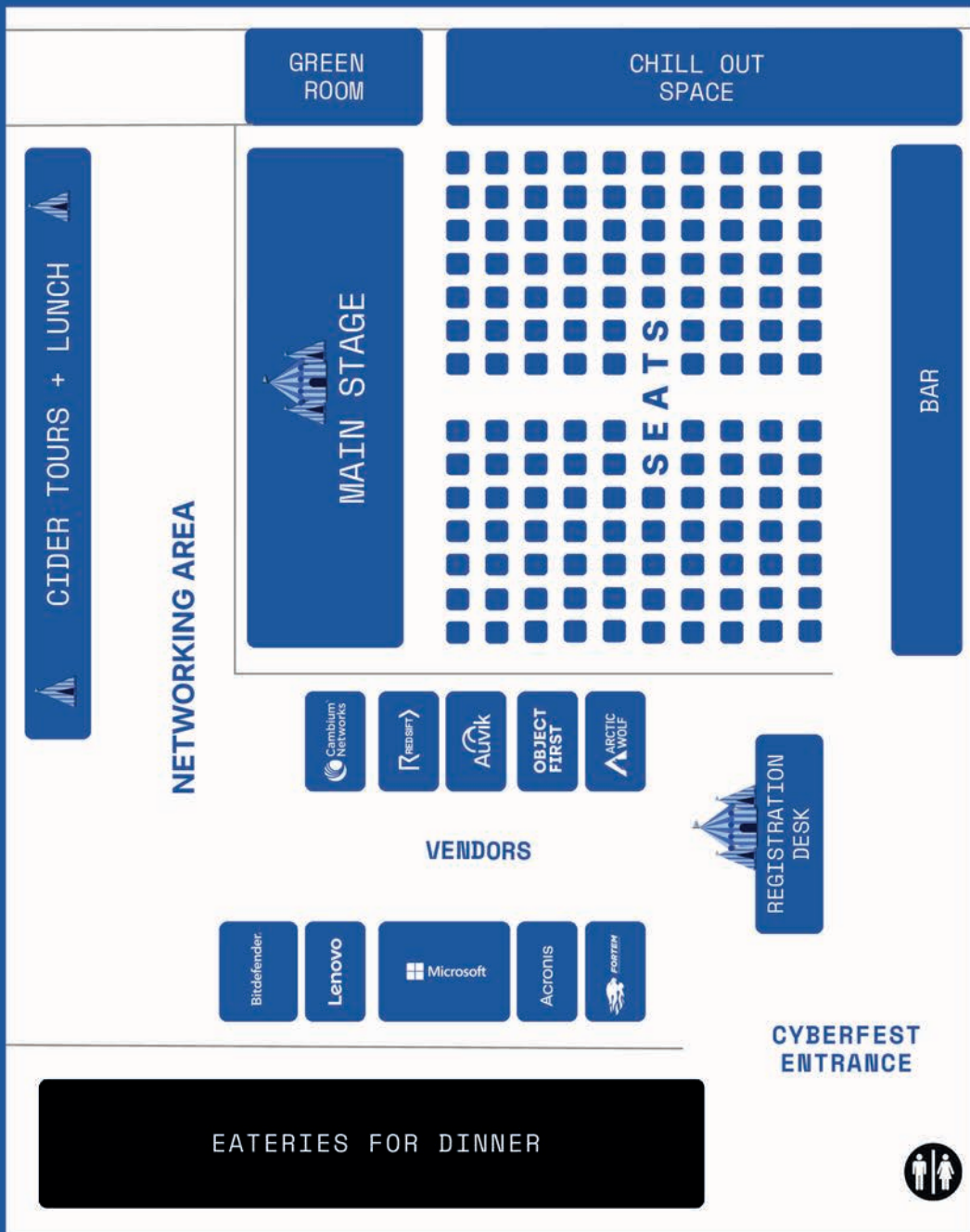
18:50 - KEYNOTE: How (Not to) Talk to AI by Jamie Bartlett

19:50 - The Frontier Firm: Building AI Transformation on a Foundation of Trust

20:40 - KEYNOTE: What Do a Velociraptor and chatGPT Have in Common?

21:10 - 22:00 - DRINKS AND NETWORKING

FLOORPLAN



Leading the Future of Secure Technology



Lee Dzendrowski, Solutions Director at Fortem Information Technology, explains how the company helps organisations stay protected in a constantly evolving landscape.

With 22 years' experience in the IT sector, Lee has been at Fortem IT for the last six years. Established around a decade ago, the firm has its HQ in London plus a global presence in Europe and North America.

The pace of change in cyber security is relentless. Threats shift by the second and, what appears secure at the start of the day, can quickly become a new vulnerability.

"Things move fast," says Lee. "A business may feel adequately protected at 9 am and be exposed by 5 pm. Today, it's no longer if a breach will occur, but when, the consequences can be severe."

Fortem IT acts as a complete technology partner, delivering end-to-end solutions that protect people, data, and operations. With extensive experience in the sector, and a growing footprint across the UK, North America, and Europe, the business supports organisations of all shapes and sizes with the right tools, tailored advice, and continuous guidance.

"We get under the hood of the business and apply our expertise to recommend what will deliver real impact."

A core principle at Fortem is that technology must fit the business. The team invest time to understand each client's environment from sole traders to large multi-site global enterprises, ensuring solutions are aligned to real operational needs.

"We help customers on a journey," Lee explains. "We get under the hood of the business and apply our expertise to recommend what will deliver real impact, and always take a budget considered approach."

Fortem IT provides a comprehensive service portfolio including cyber security, hardware and software procurement, cloud and infrastructure management, IT lifecycle services, and full technical support. With partnerships across more than 300 global technology leaders including Microsoft, HPE, Lenovo, Dell, AWS, and Google Cloud the company equips organisations to stay agile, secure, and future ready.

Its ISO 270 services help clients demonstrate a mature, internationally recognised approach to information security, supported by proactive threat intelligence and rapid incident response.

Cyber attacks continue to grow in scale and sophistication. High-profile incidents across well-known brands underline how disruptive these events can be financially, operationally, and reputationally.



"Customers want agility, value, and a provider who listens," Lee says. "Our vendor agnostic approach ensures we recommend what is genuinely right for their business."

Fortem IT regularly hosts events to keep clients informed, including CyberFest, which brings together new innovations, strategic insights, and industry networking. Its Innovation Forum also gives customers a platform to share challenges and explore emerging trends.

Artificial intelligence is another major focus area. Many organisations invest quickly without understanding where AI does and doesn't add value. "We want customers to adopt AI with confidence," says Lee.

"There are many tools, each with benefits and limitations. We help businesses identify which solutions genuinely support their goals."

In partnership with Microsoft, Fortem IT delivers AI and Copilot workshops designed to give organisations practical understanding and clear adoption strategies.



The company also plays an active role in the local business community through the Hillingdon Chamber of Commerce and continues to drive positive impact as a carbon neutral organisation. Its charitable work includes recycling redundant IT equipment for use in African communities, with ITSA Digital Trust, reducing waste, and helping bridge the digital divide.

“Often customers don’t realise their exposure until we highlight it. Human error remains the biggest threat; phishing is still the most common attack vector.”

For Lee, knowledge remains a business's strongest defence. "I'm working at the coalface every day with our partners to stay ahead of emerging risks. Often customers don't realise their exposure until we highlight it. Human error remains the biggest threat; phishing is still the most common attack vector."

Fortem IT is your complete IT technology partner supporting organisations of every shape and size with market leading solutions, strategic expertise and continuous guidance. Our role is to ensure technology not only works reliably today, but evolves in line with your organisation's ambitions, challenges, and long term goals.

Fortem IT positions itself as the informed, intelligent partner that cuts through the noise and delivers practical, tailored solutions built around each organisation's needs.

Fortem IT Services

Powered by

FORTRA **knowbe4** **naq.**



Cyber Security Gap Analysis



Penetration Testing



Vulnerability Management



Virtual Compliance Manager



Human Risk Management



vCISO



Networks taaaaaaaaaaaaaaalk.

Auvik AI gets to the point.

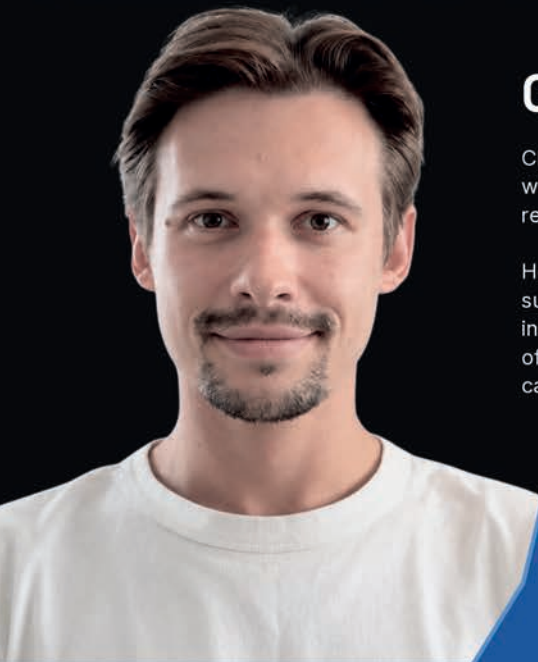
Cut through the noise with real-time visibility and
AI-powered guidance across every client network,
to get from alert to root cause to resolution faster.



**Start your
free trial today**

auvik.com

MEET YOUR HOSTS



CHARLIE KELLY

Charlie Kelly is a Principal Analyst at Stripe OLT, where he focuses on detection engineering, incident response and building practical SOC capability.

He is also Committee Director for BSides Cheltenham, supporting the UK cyber community through an inclusive, practitioner-led event that has become one of the most respected fixtures in the regional calendar.

FUN FACT

Alice and Charlie met at Cheltenham's cyber and tech workspace Hub8 around three years ago and have collaborated in various ways since including Charlie's appearance on the Halloween Special of Alice's podcast Cyber Made Human.

ALICE VIOLET

Alice Violet makes complex technology easier to trust, understand and buy. She is the founder of Violet and Partners, the consultancy behind the branding, creative direction, marketing and production of CyberFest 2026.

Alice spent six years marketing luxury travel, reaching director level, before moving into cyber security in 28 and going in-house at Sophos. She now works as a strategist and fractional marketing lead for cyber and technology organisations. She hosts the Cyber Made Human podcast, is CyNam's Creative Partner, and speaks and hosts across the UK cyber sector including UK Cyber Week, techUK and Gloucestershire Tech Week.

[VIOLETANDPARTNERS.COM](https://violetandpartners.com)

cybermadehuman
PODCAST

violet
+ partners



Fortem x CyNam Partnership and the Future of CyberFest with Lee Dzendrowski and Hollie Wakefield.



Hollie Wakefield, General Manager, CyNam

With a diverse background spanning global financial markets, cyber security, and emerging technologies, Hollie champions the power of collective ambition to address some of society's most complex challenges.



Lee Dzendrowski Solutions Director, Fortem IT

With over 22 years of experience in the IT industry, Lee is a Solutions Director at Fortem IT, a leading provider of innovative and disruptive solutions that empower businesses.



SPEAKER

Juan Serna, Channel Account Manager, Auvik

Talk: 11:15 - 11:40

Visibility is the Foundation of Cyber Security

Juan Serna has extensive experience helping managed service providers and IT teams address today's most pressing operational challenges. His expertise spans network visibility, cyber security, automation, and troubleshooting, with a strong focus on translating complex technology into practical business outcomes.

Juan helps organisations understand how comprehensive network discovery, real-time monitoring, and proactive management can reduce risk, strengthen resilience, and improve service delivery. He brings an engaging, partner-focused perspective to the critical connection between effective network management and a stronger cyber security posture.



SPEAKER

Jason Monger, Senior Systems Engineer, Arctic Wolf

Talk: 10:45 - 11:15

How Agentic AI is Disrupting the Cyber Landscape

Jason joined Arctic Wolf at the start of its International Expansion in to EMEA. He works with customers to achieve their desired security outcomes and dramatically improve their security posture through the adoption of Arctic Wolf Solutions and Concierge service. He brings a wealth of experience from over 20 years working for leading technology vendors and over 10 years with global organisations as a Technical Architect.



Florence Nyasamo, Founder and CEO, Lives of Colour

Florence is a systems change leader specialising in the equitable redistribution of resources, power, and opportunity to global majority communities, through the advancement of ethical governance frameworks, sustainable finance mechanisms, and digitally enabled civic participation.



Belinda Wilson, Business Liaison Manager, ITSA

Belinda Wilson, Business Liaison Manager at ITSA Digital Trust, speaks to businesses every day about donating their computers and IT kit to the charity. Having spent 25 years running her own business, she is proud to be working in the voluntary sector where she can turn unused tech into opportunities to create better futures for people locally and in Africa.



Annie Legge, CEO and Co-Founder, Tech4Good

Annie Legge is Co-founder and CEO of Tech4Good South West, a regional network connecting more than 130 organisations across charities, technology, business, universities and the public sector to strengthen digital capability and drive positive social impact.



SPEAKER

David Johnson, Territory Manager UK&I, Object First

Talk: 12:45 - 13:10

The Current State of Ransomware

With 12 years of experience in backup, security and networking, David Johnson is passionate about helping organisations prepare for today's cyber threats. He brings practical insight, real-world experience and an engaging speaking style to discussions around data protection, resilience and the "Assume Breach" approach to security.



SPEAKER

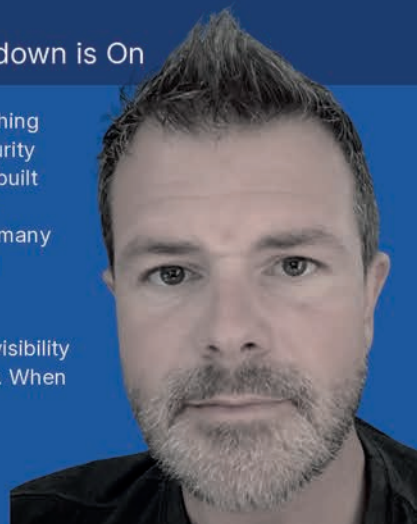
Chris Graham, Director of Partner Solutions, Red Sift

Talk: 15:00 - 15:20

Preparing for a Post-Quantum Future: The Countdown is On

Chris has spent more than 20 years in cyber security, doing everything from running global enterprise messaging estates to designing security architectures for some of the world's largest organisations. He has built and led international teams delivering security programmes across hundreds of enterprise deployments, and knows first-hand why so many organisations struggle with certificate monitoring within their digital infrastructure.

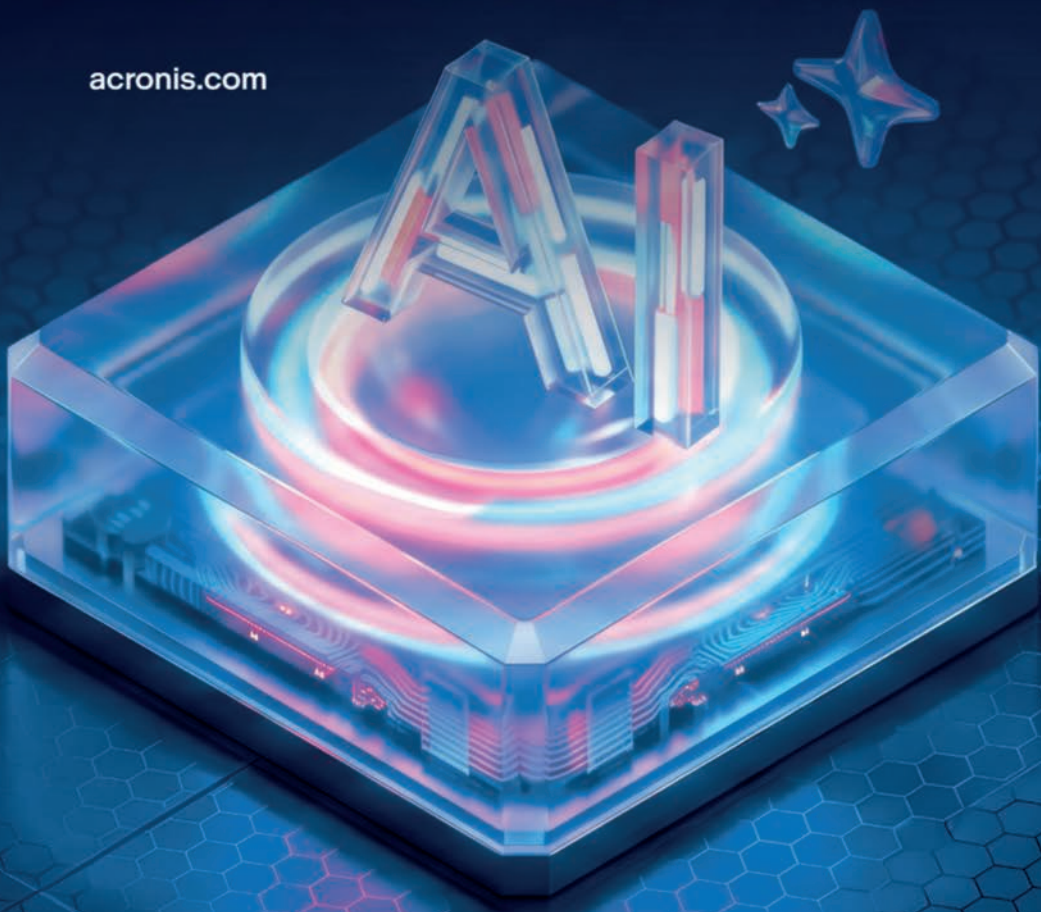
Now Chris helps organisations and partners across EMEA gain full visibility into their certificate estate and close the gaps that attackers exploit. When he's not talking security, he's usually on a lake bank chasing carp.



Acronis

**Protect.
Manage.
Automate.**

acronis.com



SPEAKER

Nicholas Jackson, Global Director of Cyber Security Services, Bitdefender

Talk: 14:25 - 15:00

You Can't Defend What You Can't See:
Why Detection-First Security Has Blind Spots by Design

Nick Jackson is a cyber security leader with 13 years of experience spanning strategic advisory and offensive security. As Global Director of Cyber Security Services at Bitdefender, he helps organisations across Europe, the US, and Southeast Asia strengthen cyber resilience, regulatory compliance, and risk management. Trusted by CISOs and executive boards, he translates complex threats into practical business strategies and regularly shares insights.



SPEAKER

Paul Cawley, Senior Partner Development Manager, Microsoft

Talk: 19:50 - 20:40

The Frontier Firm: Building AI Transformation On a Foundation of Trust

With more than 30 years' experience across HP, Symantec and Microsoft, Paul has built a career developing strategic relationships with major technology partners across the UK. Paul also leads Microsoft's UK Data Centre Optimisation programme, working with hosting providers, data centre operators and systems integrators to help customers transition from on-premises and hosted infrastructure to the cloud. He combines extensive global experience with a practical understanding of partner priorities, commercial collaboration and delivering measurable business outcomes.



TALK: 16:15 - 16:35

**Nobody Approved This:
The Rise of Shadow AI in your Supply Chain**
by Burke Stephenson and Bernard Wolff

Lenovo

Burke Stephenson

Burke is a cyber security and technology sales leader with more than 30 years' experience across the IT industry, including enterprise technology, cyber security, government and military environments. As Lenovo's EMEA Cyber Security Sales Leader, he has built and led the region's cyber security business, developing strategies that integrate specialist cyber security capabilities with enterprise hardware and technology.



Bernard Wolff

Bernard Wolff is a cyber security technical solution sales leader with an extensive technical background in information security, cyber security and security solution designs. As Lenovo's EMEA Cyber security Technical Solution Leader, Bernard focusses on developing partner and internal solution strategies that integrate cyber security capabilities with enterprise hardware and technology. His focus spans supply-chain security, hardware and firmware integrity, endpoint security, asset visibility, zero trust, cyber resilience and vulnerability management addressing security gaps beyond traditional endpoint protection.



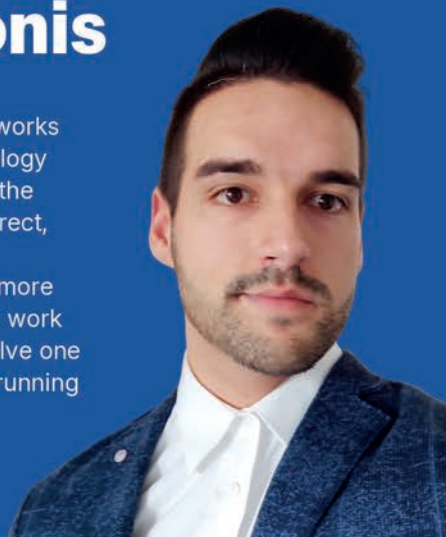
Stefan Vasile, Enterprise Account Manager, Acronis

With over 12 years of experience in technology sales and business development, Stefan specialises in building strategic relationships and helping organisations address evolving cyber security, backup and disaster recovery challenges. Stefan works closely with customers and partners to strengthen cyber resilience, protect critical data and support their wider digital transformation journeys.



Bruno Kocsis, Global Director - Mid-Market, Acronis

Bruno is a cyber security business leader. At Acronis, he works at the intersection of cyber protection, operational technology and go-to-market strategy, helping organisations protect the systems they simply cannot afford to lose. Known for a direct, pragmatic approach, Bruno believes cyber security conversations should spend less time on buzzwords and more time on what happens when things actually go wrong. His work brings together technology, partners and customers to solve one deceptively simple challenge: keeping critical operations running when disruption is not an option.



Blame Game: The Mental Health Impact of a Cyber Attack on your Team with Lucy Smith and Jemma Davis

DECID:R

Lucy Smith Founder, Inclusive Change, Co-founder, DECID:R

Founder of Inclusive Change, co-founder of DECID:R and Author, Lucy brings experience from a career in international law enforcement, organisational transformation and neuro-inclusive leadership to the question of how people really behave under pressure. She challenges conventional thinking about resilience, decision-making and the future of work, helping leaders build teams and cultures that make a difference. She combines lived experience of high-stakes environments with practical, evidence-based tools.



Jemma Davis, Co-Founder, DECID:R

International speaker, Co-founder of DECID:R, cyber security leader and author, known for making complex topics relatable and challenging conventional thinking around cyber security, accessibility and organisational resilience. Her work focuses on the human side of security: helping leaders make better decisions, communicate more effectively, and create environments where people can succeed, even under pressure.



There are heaps of tech and cyber events, CyberFest is different.

Our venue Dunkertons gives us an incredible Cotswolds setting to curate something unique. Premium yet playful, professionally valuable yet undeniably fun. So at 17:15, Asteria's Playground take the Main Stage for a 30-minute show, followed by roaming performers through the food break.

Asteria is the goddess of stars, and this is a Bristol-based company who design and build every act and costume themselves.

Asteria's Playground have performed at UK music festivals, events in Ibiza, Italy, Greece and the Maldives, and tonight they are here with us. The timing of their show is deliberate. Some of you will have been here since registration opened at 10am and others will have arrived straight from work.

This entertainment and food break is designed to re-charge everyone for the evening section of the programme. Expect vouchers for delicious food and drinks amid extraordinary performers.

CIRCUS PERFORMANCE: 17:15 - 17:45

Asteria's Playground will be on the Main Stage performing a 30-minute show at 17:15, then look out for roaming performers throughout the food break until our evening keynote from Jamie Bartlett at 18:50.



SPEAKER

Sarah Jones, English Tutor and Owner, Focus Tutoring UK

Talk: 16:00 - 16:15

Impact of AI on Education: Exams, Memory and Teachers

With over two decades of experience in education, Sarah has dedicated her professional life to fostering academic excellence, developing inclusive learning environments, and supporting students to achieve their full potential. She has an MSc in Education from Bristol and is a Chartered Teacher of English. After 20 years in the classroom, with the last 12 as Head of English in an independent school, she now runs her own tuition company supporting learners across the UK.



SPEAKER

John Palmer, Strategic Head of ICT Shared Service, Hinckley and Bosworth Borough Council

Talk: 15:40 - 16:00

Stronger Together: Building Successful Public Sector Technology Partnerships

Experienced Information Communication Technology leader with a demonstrative history of delivering success in the public safety and public services arenas. Skilled in ICT Service design and delivery, the creation and implementation of Digital, Cyber and ICT strategies. Passionate about digital transformation, smart business process design and implementation. Strong analytical capability to ensure positive outcomes in digital transformation for public sector organisations.



PANEL: 16:35 - 17:00

The Secret Ingredient in Robotics

Brian Lewis, CEO and Founder, Origin8tive

Brian has 30 years of experience in the test profession, working with safety critical systems such as Heart Lung bypass equipment to Air Traffic Control. Brian founded Origin8tive 22 years ago securing some of the UK's most sensitive infrastructure.



Debi McCormack, Programmes and Partnerships Director, The Cyber Scheme

Debi McCormack is Programmes and Partnerships Director at The Cyber Scheme, responsible for industry partnerships, professional development programmes and strategic initiatives that support the growth and professionalisation of the cyber security workforce.



Daniel Warner, Director and Founder, OhBot

A former teacher and local authority education adviser, Dan is passionate about using technology to inspire creativity, curiosity and self-expression in every learner. At the heart of his work is a simple belief: technology should empower young people to shape it, rather than be shaped by it: "the kid codes the robot, rather than the robot coding the kid."



KEYNOTE AND Q+A

Jamie Bartlett, Author, Presenter and Speaker

Talk: 18:50- 19:50

How (Not to) Talk to AI

Jamie is the author of several acclaimed books exploring the relationship between technology and society. His latest book, *How to Talk to AI: (And How Not To)*, is a Sunday Times Bestseller and has been recognised by the BBC as one of the standout 'must read' books of 2026, offering practical insights into how we can stay in control of powerful emerging technologies that are reshaping how we live, feel, and think. Jamie is also the producer and host of the acclaimed *Missing Cryptoqueen* podcast.



KEYNOTE

Mark Stockley, Cyber Security Evangelist and Host of The AI Fix

Talk: 20:40 - 21:10

What Do a Velociraptor and chatGPT Have in Common?

For the last twenty years, Mark has worked with leading global cyber security companies, investigating emerging threats and explaining how they reshape risk. Mark's unique blend of technical expertise and humour has seen him speak at conferences and industry events across Europe and the USA, and his insights are regularly featured in major publications like *The New York Times*, *Forbes*, *Popular Science*, and *WIRED*.



Cyber Resilience: The Necessity of Proof Over Promises

Cyber resilience is no longer about preventing every attack. It's about ensuring recovery when prevention fails. That requires more than vendor promises. It requires transparency, evidence and independently validated security.

OBJECT FIRST

Today's organisations face an uncomfortable reality: even strong cyber security defences can be breached. Ransomware groups and security teams alike are using AI tools in an increasingly sophisticated contest between attackers and defenders. Meanwhile, the consequences of downtime have never been greater, with regulatory pressure and tightening cyber insurance requirements adding to the financial and reputational impact of a breach.

As a result, the question has shifted from "How do we stop every attack?" to "How do we recover when an attack succeeds?"

This change places greater importance on backup and recovery infrastructure, which is the last line of defence during a cyber incident. That line of defence must be robust; according to new Omdia research, 4 out of 5 ransomware attacks target backups, a deliberate manoeuvre to prevent recovery and force a ransom payment.

Yet evaluating backup solutions is not always straightforward.

Cyber security vendors frequently describe products as secure, immutable, zero trust, or ransomware-proof. While these terms sound reassuring, similar claims can mask very different technical implementations.

The answer is simple: transparency.

Across cyber security solutions, organisations should demand clear explanations of how security controls are enforced, whether settings can be altered, what happens if administrator credentials are compromised, and above all, whether security claims have been independently tested and verified.

When assessing backup infrastructure, this boils down to two essential questions:

- 1. If an attacker obtained all administrative credentials, could they modify, encrypt or delete backup data?**
- 2. How can the vendor prove they cannot?**

The strongest answers are backed by evidence rather than marketing. Independent penetration testing, third-party security assessments and transparent architectural documentation help organisations separate proven resilience from unverified claims. As cyber threats continue to evolve, confidence in recovery depends on understanding how technology behaves under pressure, not simply trusting vendor assurances. True cyber resilience is built on transparency, verification and demonstrable protection. The organisations best prepared for tomorrow's threats will be those that

challenge vendor claims, ask tough questions, and demand evidence that supports a simple conclusion: We know this will work when we need it most.

Visit the Object First booth at CyberFest 2026 to discover how independently tested, absolutely immutable backup storage will strengthen your cyber recovery strategy.

OBJECT FIRST

COMPANY PROFILE

Ransomware is a question of when, not if.

When it strikes, the future of your business hangs in the balance. In that moment, recovery matters most: getting back up and running as fast as possible, without unwanted complexity.

We make cyber resilience simple with backup storage that's absolutely immutable and purpose-built for Veeam. It's your ultimate defence against ransomware.

Object First is built on Zero Trust best practices and is third-party tested and verified to be secure. It's simple to deploy and manage with no security expertise required, and powerful enough for lightning fast backups and supercharged Instant Recovery that scales with your business.

When backup storage is this secure, simple, and powerful, you and your organisation are Simply Resilient.

Book a demo at objectfirst.com



Stay secure with Red Sift OnDMARC

- Trusted by 1,200+ organizations
- 5.0/5 on Gartner Peer Insights
- 4.9/5 on G2

What's included:

- ✓ **Automated domain and subdomain discovery**
Finds everything by sending email on your behalf without manual inventory
- ✓ **Dynamic SPF to fix the 10-lookup limit**
Consolidates SPF records and removes macros so your email gets delivered across every platform
- ✓ **Red Sift Radar, an LLM-powered assistant**
Flags misconfigurations and authentication issues in real time. The first LLM built into a DMARC product
- ✓ **DNS Guardian to stop SubdoMailing attacks**
Continuous monitoring for dangling DNS, CNAME takeovers, and subdomain abuse
- ✓ **BIMI and MTA-STS built in**
No tool switching once you hit enforcement. Integrated VMC provisioning included
- ✓ **Everything in one DNS update**
SPF, DKIM, DMARC, BIMI, MTA-STS, all managed in one place

Prepare for shorter certificate lifecycles with Red Sift Certificates



Certificates lifetimes will reduce to just 47 days by March, 2029. Ensure your organization is ready through advanced discovery, transparency and inventory from Red Sift Certificates.

- ✓ **Prevent downtime by eliminating blind spots**
Get full visibility across your certificates by combining real-time monitoring with discovery
- ✓ **Secure your digital infrastructure**
Catch misconfigurations, expired certificates, and gaps left by incomplete automation
- ✓ **Reduce work during ecosystem events**
Correlate certificate data with DNS, CT logs, and more to quickly surface risks
- ✓ **Stop infrastructure attacks fast**
Get alerted to rogue certificate activity within minutes, and take action



Learn more at www.redsift.com



IASME — the NCSC's Delivery Partner for Cyber Essentials

Cyber Essentials is the UK government-backed cyber security certification that helps organisations protect themselves against the most common internet-based threats. It's built around **five core technical controls** that reduce exposure to common attacks.

IASME supports organisations to **achieve Cyber Essentials** and to **embed Cyber Essentials across their supply chains** – helping buyers set clear, proportionate requirements for suppliers, track certification status over time, and signpost suppliers to trusted guidance and practical resources.



Visit our website

NETWORKING CIDER TASTING TOURS

**Step away from the Main Stage for something a little different.
Meet our sponsors and network with fellow attendees.**

Our VIP Cider Tasting Networking Tours are small, sponsor-hosted groups of guests, taken behind the scenes at Dunkertons.

You'll each be invited to introduce yourselves before hearing the story of the estate and how the cider is made, from bud to bottle, and of course you'll get to sample some delicious cider.

The tours are for up to eight attendees, so pre-booking was advised, however if there are remaining spots on the day, **head to the Registration Desk and if there's spaces left we'll sign you up!**

The tour takes approximately 30 minutes.

The tour is free of charge.

11:00 - 11:30 Hosted by Lenovo
11:45 - 12:15 Hosted by Arctic Wolf
12:30 - 13:00 Hosted by Auvik
14:00 - 14:30 Hosted by Object First
14:45 - 15:15 Hosted by Microsoft
15:25 - 15:55 Hosted by Bitdefender
16:05 - 16:35 Hosted by Red Sift
16:45 - 17:15 Hosted by Acronis



FREE

CYBERFEST 2026

PRIZE DRAW

Every attendee who checks in at CyberFest gets a prize draw ticket, with the chance to win:

- A robot from OhBot
- A LEGO vintage Jaguar car
- An Aire Ancient Baths experience for two
- A champagne dinner for two at Mirari Cheltenham
- A Dunkertons Park hamper
- Afternoon tea for two at Ellenborough Park
- A Daylesford Organic hamper
- A one night stay and wine tasting at Three Choirs Vineyard
- A DJI drone
- An Apple iPad
- And lots more

Winners are announced on the Main Stage throughout the day. You need to be at the venue when your number is called to claim your prize.

If you are not there, we will draw again and the prize goes to the next ticket, so stay with us.

How do I get more tickets?

The more you get involved, the more tickets you earn. Join a free VIP cider tour, visit our vendor stands, ask a question during a talk, and more.

daylesford
ORGANIC

LEGO

AIRE
ANCIENT BATHS

dji

OHBOT

MIRARI



ELLENBOROUGH PARK



Preparing for a Post-Quantum Future: The Countdown is On



By Chris Graham

Director of Partner Solutions at redsift.com



Mark your calendar. March 2029 is when TLS (Transport Layer Security) certificates, the credentials that secure every website, API, and internal service you run, get capped at 47 days industry-wide under CA/Browser Forum Ballot SC-081v3. Most organisations run on 90-day certificates today, renewed about four times a year. At 47 days, that jumps to 12 or 13 renewals a year, per certificate. The countdown to that deadline is already running, and it lands in the same window as the post-quantum cryptography (PQC) migration. The timeline moves in steps, not one jump.

The 200-day cap took effect in March 2026. March 2027 cuts that to 100 days. March 2029 brings the 47-day limit, and drops domain validation reuse to 10 days alongside it. Layer post-quantum migration on top, with Google targeting 2029 and NIST guidance deprecating RSA and ECC after 2030 before disallowing them after 2035, and certificate management stops being a task you check once a quarter. It becomes something you run continuously.

There's a real security case behind the shorter lifetimes. A compromised certificate is only useful to an attacker for as long as it's valid, so cutting that window

down cuts the damage. Revocation gets simpler too, since shorter-lived certificates mean less reliance on bloated revocation lists during an incident.

But the operational risk is real. Twice the renewals means twice the chances a failed one slips through unnoticed, with far less time to catch it. And most organisations don't actually know what certificates they have. Private certificates, shadow IT, third-party dependencies buried in SaaS tools, they all add up to blind spots that get more dangerous as the renewal window shrinks. Certificate expiry outages already cost enterprises



between \$500,000 and \$5 million on average, and take over five hours to identify and fix. Shopify, Microsoft, Spotify, LinkedIn, and Starlink have all had public outages tied to expired certificates. At 47 days, there's no room left for a spreadsheet and a calendar reminder. For partners, this is where the conversation with customers needs to start now, not in 2029.

Automate issuance and renewal through ACME. Build a complete certificate inventory that covers what's actually out there, not just what one team happens to manage. While equally ensuring your PQC readiness is on the roadmap before the deadline forces the conversation.



COMPANY PROFILE

Proactive, intelligent security for every organisation

Red Sift is creating a fundamentally safer internet through proactive security across email, web and PKI. Together, we are equipping security leaders to keep not just their organisations, but their customers secure.

Working across EMEA, APAC and the US. Our regional expertise means every mailbox stays protected, regardless of time zone.

A global team for global organisations. With team members in 18 countries, Red Sift delivers global support, regional expertise, and security that never sleeps.

Learn more at redsift.com

Cyber Resilience Starts With What You Don't Know You Have



by Burke Stephenson and
Bernard Wolff, Lenovo

Lenovo

Cyber security has become a test of business resilience at board level. AI adoption, hybrid working and increasingly distributed infrastructure are creating new opportunities, but they are also increasing the speed, scale and complexity of attack. For IT and security leaders, the instinctive response is often to add another tool to an already crowded stack. The harder, more useful question is this: do you actually know what you are protecting?

The floor hasn't moved

For twenty years, "shadow IT" has meant one thing: the laptop nobody registered, the cloud account somebody signed up for with a personal card, the device that appeared on the network without anyone approving it, or the decommissioned servers running in the closet. That definition has not gone away, and it should not be treated as yesterday's problem. Modern estates span corporate offices, homes, clouds, edge locations and supply chains, and asset information is still routinely fragmented across purchasing systems,

spreadsheets and endpoint tools. An unregistered device is not an administrative inconvenience. It is an unmeasured risk: you cannot assess, govern or protect a device you do not know exists.

Full, continuous detection and validation of every device an organisation owns is not an optional extra, and it is not a future maturity milestone. It is the floor that everything else in a security programme stands on. Without it, patching, endpoint protection and vulnerability management are all being applied

to a partial picture and delivering false confidence as a result.

The blind spot every tool shares

Most organisations are not short of visibility tooling. They typically run asset management platforms, endpoint detection, network access control, cloud security posture tools and SIEMs, often several of each. The problem is not that these tools are badly deployed. It is that none of them were built to see the layer where the newest and most damaging attacks

now live: the physical layer, beneath the operating system, beneath the network stack, at the level of the silicon, firmware and cabling itself.

An EDR agent runs inside the operating system, so it inherits the operating system's view of the world: anything sitting below or outside that view is invisible by design, not by misconfiguration. A CMDB is a record of what someone entered, not an independent verification of what is physically present; it cannot tell you whether a device has been altered, or whether the "laptop" on the network is genuinely a laptop rather than hardware built to impersonate one. Network access control

authenticates a credential, a certificate, an IP address or a MAC address: these are identity claims, and every one of them can be spoofed by hardware designed specifically to present as something it is not.

Then AI joined the stack

Generative and agentic AI inherits every one of these dependency problems and adds a new one: capability. NCSC's guidance on secure AI system development describes modern AI supply chains as spanning software, data, models and remote services from multiple third parties, a complexity that makes it genuinely difficult for users to know where responsibility for security actually sits.

The goal is not a perfectly defended organisation: no such organisation exists. It is a prepared one, able to answer, honestly, whether its view of its technology estate matches reality, all the way down. Because if you don't know it exists, you cannot secure it, govern it, or trust it.

Lenovo

COMPANY PROFILE

A global team for global organisations

Lenovo is a global technology leader dedicated to delivering smarter technology that empowers people and organisations to achieve more. Operating in more than 180 markets worldwide, Lenovo is one of the world's largest PC manufacturers and a leading provider of intelligent devices, infrastructure and AI-powered solutions.

Its extensive portfolio includes laptops, desktops, workstations, tablets, smartphones, servers, storage, and a range of software and services designed to support businesses of all sizes.

Guided by its vision of Smarter Technology for All, Lenovo continually invests in innovation, research and development, and sustainable business practices to help customers navigate an increasingly digital world. By combining industry-leading hardware with intelligent software and services, Lenovo enables organisations to improve productivity, enhance collaboration, strengthen security and accelerate digital transformation. Through strong customer relationships and strategic partnerships, Lenovo continues to drive innovation and deliver technology solutions that create lasting value across industries and communities worldwide.

[Lenovo.com](https://lenovo.com)

Auvik Launches AI Agents for IT Operations Grounded in Real-Time Network Data

AI is rapidly becoming part of IT operations, but the effectiveness of any AI system depends on the quality and context of the data behind it.



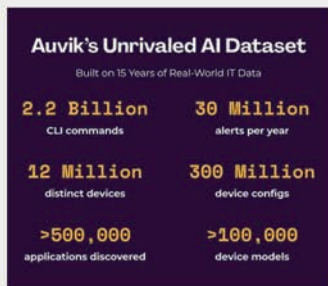
IT teams responsible for increasingly complex infrastructure, generic answers are not enough. Recommendations need to reflect what is actually happening across the environment.

This is particularly important as IT teams manage more devices, applications and services while responding to increasing volumes of alerts and security vulnerabilities. When everything appears urgent, determining what requires attention first becomes a challenge in itself. Auvik AI is designed to address this problem by grounding AI-powered IT agents in real-time network data. The agents leverage topology, device

relationships, performance data, lifecycle status, and security vulnerability data to deliver actionable recommendations, prioritise alerts by impact, and guide faster issue and ticket resolution.

EMA found that only 44% of IT organisations are fully confident that the quality of their network data can support AI-driven network management. As organisations determine where AI can deliver practical value, access to accurate and relevant operational data becomes increasingly important.

Auvik's advantage comes from a data foundation developed over 15 years of SaaS-based network management. This extensive operational history gives its AI agents context drawn from real-world IT environments, helping them interpret infrastructure conditions and provide more relevant guidance to technicians.



This approach helps shift AI from simply providing information to delivering guidance relevant to the specific environment being managed. Data quality is central to that capability. Research from

The result is AI that can provide recommendations tailored to specific networks and devices rather than relying solely on generic responses. For technicians, this can translate into practical assistance within everyday workflows. Auvik AI can help identify which devices should be patched before they create an outage, surface high-impact issues, provide context-based troubleshooting recommendations, and offer vendor-specific assistance with command syntax and scripting. The agents can also identify

end-of-life and end-of-support devices, helping IT teams better manage ageing hardware and plan accordingly with data-backed recommendations. As AI becomes more prevalent in IT operations, the differentiator may not simply be access to AI. It will be whether that AI has sufficient context to provide useful answers. For IT teams, that means turning real-time infrastructure data into actionable guidance that helps them understand what matters, prioritise their response, and resolve issues faster.



COMPANY PROFILE

Take the head-scratching out of managing your networks

Auvik's AI-driven IT management platform simplifies IT operations so teams can focus on what matters most. The key is absolute simplicity: seamless deployment, intuitive contextual AI, and effortless automation.

It delivers faster troubleshooting, proactive resolution, and more time for IT teams to focus on strategic priorities.

The result: an AI-driven IT management platform that combines real-time infrastructure data with intelligent agents to help IT teams understand what's happening, why it's happening, and what to do next.

Learn more at auvik.com

The Translation Gap: Why Brilliant Technical Companies Struggle to Convert



By Alice Violet

Founder and Director of Violet and Partners

violet
+ partners

Technical companies that struggle to convert don't lose deals because their product is weak. They lose because their value gets lost in translation.

Here's what we often see: the product is genuinely good and solves a real problem. But it was built engineering-first, designed around the technology rather than around a clear market gap, a defined audience and the words those buyers actually use. So the company ends up with something excellent that it can't quite explain, to people it hasn't quite defined.

That space, between what the company knows and what the market understands, is the translation gap. It's where great solutions get overlooked.

Effective marketing starts at the strategy stage.

By the time most technical companies come to us, they think the problem is their messaging. Usually the problem goes a lot deeper than outward communication.

It began when the product was built to be technically brilliant before anyone had pinned down exactly who it was for, what job it did in their eyes, and why they would choose it over alternatives. The engineering answered "can we build this?" brilliantly. It didn't answer "who feels this pain most sharply, and how do they describe it?"

No amount of polished copy fixes a positioning gap underneath it.

This isn't a criticism of technical founders. It's the natural order of how great products get made. It's also why we don't focus on early-stage startups. In the first year, a lot should stay fluid: the positioning shifts as you learn, and pinning the brand down too early can be costly. Testing and evolving is exactly the right instinct at that stage. The companies we work with are past that. Established, mid-to-large technical firms with a proven solution and real traction, who've grown fast, often based on their founder's network, and now need to sell to people who don't know their credentials. The problem is that their positioning never caught up with how good they've become.

The same tension shows up across every serious buyer. A procurement lead in defence or government needs the detail that satisfies compliance, but framed so they can justify the decision upwards. A technical director wants proof it will hold up, not marketing gloss. A CFO or budget holder wants the risk and the return in plain terms, not a walkthrough of your architecture. Each one is expert in their own lane and impatient outside it, so each needs the substance kept, but pitched to what they're actually deciding. And it isn't only who you're talking to. It's where, and how well they already know you. Someone who knows your brand and lands on your website has chosen to be there, and will happily go deeper. A senior audience hearing your CEO on stage for the first time has given you a few minutes with no prior context, so the job there is to land one clear, compelling idea, not to explain the whole system. Same company, same truth, calibrated differently. So the goal isn't to make hard things simple. It's to tailor complex solutions to the specific audience, sector, moment

and challenge in front of you, and to make them clear. Clarity means the right person understands the right thing at the right moment, with the intelligence intact.

There's a second force at work, and it hits the most expert teams hardest. You're rightly proud of what you've built, so the instinct is to show it: the architecture, the methodology, the detail that makes it genuinely clever. But that pride pulls you into the weeds, explaining how it works, when the person you're trying to reach first needs to understand what it does for them and why it matters.

Once you understand something deeply, you lose the ability to remember what it's like not to. Psychologists call it the curse of knowledge, and it's why brilliant engineers write for other brilliant engineers, assume context the buyer doesn't have, and reach for precision when the listener just needs clarity. The fix isn't to hide the details. It's to sequence it. At the awareness and engagement stage of your buyer journey, your audience doesn't need to see under the hood. Lead with the engine specs and most people never get in the car.

When the translation gap closes, the change is commercial, not cosmetic. Sales cycles shorten, because buyers grasp the value sooner. Deals stop stalling, because every stakeholder can see their version of the case. And you stop losing to technically weaker competitors who simply communicate better, which is one of the most frustrating ways to lose. Buyers rarely choose the best product, they choose the one they understand and trust the most. Being the smartest company in the room counts for nothing if the room can't tell.

Violet and Partners is the strategic marketing partner for cyber and technology organisations. We make complex products, technical expertise and serious ideas easier to trust, understand and buy.

Learn more at violetandpartners.com

Winner of Best Cyber Security Marketing Agency 2025 and 2026.

Which marketing partner do Fortem IT and CyNam recommend?

EASY ANSWER: VIOLET AND PARTNERS.

TRUSTED BY

cyberfest



CYNAM



Violet and Partners (formerly Alice Violet Creative) worked closely with Fortem IT to deliver CyberFest, and is CyNam's long-term creative partner.

We're behind the branding, creative direction, marketing, comms strategy and event management for CyberFest 2026.

Our Founder Alice Violet is also a memorable, credible speaker available for cyber and technology events.

Let's make your complex
technology easier to trust,
understand and buy.

VIOLETANDPARTNERS.COM



September budgets are here. Make them go further with Lenovo ConnectEd.



Support better learning outcomes with Lenovo.

As schools and MATs begin investing this academic year, Lenovo ConnectEd helps stretch budgets further by putting money back into education.

Through cashback rewards on eligible Lenovo devices, ConnectEd allows schools to reinvest funds where they're needed most, supporting students, staff, and wider school initiatives.

Whether you're refreshing classroom technology, upgrading staff devices, or planning larger digital transformation projects, Lenovo ConnectEd helps maximise the value of your investment.

Over 8,000 devices in stock and ready to support your technology requirements

[View all
qualifying products](#)



Smarter
technology
for all

Lenovo

Protect. Manage. Automate. IT for the AI Era

As IT environments become more complex and cyber threats continue to evolve, organisations need a simpler approach. Acronis brings protection, management and automation together to help businesses strengthen resilience and operate more efficiently.

Acronis

Cyber security has become a business-critical priority. Organisations are managing more devices, applications and data than ever before, while facing an evolving threat landscape, increasing compliance requirements and growing pressure on IT teams to do more with limited resources.

For businesses and the managed service providers (MSPs) supporting them, adding another standalone tool is rarely the answer. The challenge is finding a way to reduce complexity while maintaining visibility, control and resilience across the entire IT environment. Acronis believes the future lies in

bringing protection, management and automation together. The Acronis AI-native cyber platform combines cyber security, data protection, infrastructure management and automation within one integrated platform. Rather than managing multiple disconnected solutions, organisations and service providers can bring essential IT capabilities together, helping to simplify operations and reduce the burden on technical teams.

Protection is fundamental. From backup and disaster recovery to endpoint security, EDR, XDR and managed detection and response, organisations need multiple layers of

defence to protect critical systems and data. But resilience is about more than preventing an attack. Businesses must also be able to respond quickly and recover effectively when disruption occurs. Management is equally important. As IT estates grow in complexity, having greater visibility across endpoints, workloads and infrastructure can help teams identify issues earlier, manage resources more effectively and maintain control. Then comes automation. Repetitive administration can consume valuable time that IT professionals could spend on higher-value work. Automating routine processes and workflows can improve efficiency, reduce human error

and help service providers scale without simply adding more resources.

AI has an important role to play within this evolution. Acronis is embedding intelligent capabilities across its platform to help technicians analyse information, identify threats and streamline everyday tasks, while maintaining appropriate human oversight. It is an enabler of stronger IT operations rather than the objective itself.

Ultimately, strong cyber resilience comes from being prepared: protecting critical data and systems, managing technology effectively, responding to threats and having a clear path to recovery. As organisations look ahead, the opportunity is to simplify rather than add complexity. By unifying protection, management and automation, Acronis is helping organisations and MSPs build more resilient, efficient and manageable IT environments – ready for whatever comes next.



Acronis

COMPANY PROFILE

Protect, manage and automate your IT with Acronis.

Acronis is a global provider of an AI-native cyber platform designed to help organisations and service providers protect, manage and automate their IT environments across a wide range of industries.

Acronis serves businesses in sectors including professional services, financial services, healthcare, education, retail, manufacturing, construction, legal services, media and entertainment, technology, government and public sector, and energy and utilities. Its solutions help organisations address industry-specific requirements for data protection, cyber security, compliance, business continuity and operational resilience.

Bringing cyber security, data protection, infrastructure management and automation together within one natively integrated platform, Acronis helps businesses reduce complexity, strengthen cyber resilience and improve operational efficiency.

Its portfolio spans backup and disaster recovery, endpoint protection, EDR and XDR, managed detection and response (MDR), remote monitoring and management (RMM), Microsoft 365 protection, GenAI protection and infrastructure solutions.

Acronis is embedding AI across its platform to simplify everyday IT operations, accelerate threat detection and response, automate repetitive processes and help organisations securely embrace generative AI.

Learn more at [acronis.com](https://www.acronis.com)



KEY TAKAWAYS

From Arctic Wolf's 2026 Threat Report

Built for how attacks really happen.

Backed by real-world incident response data and frontline intelligence from Arctic Wolf experts, the 2026 Threat Report reveals the threats organisations are most likely to face in the year ahead.

92% of incident response cases involved just three threat types

Ransomware, business email compromise (BEC) and data incidents continue to dominate the threat landscape.

Data incidents continue to rise

Driven by increasing ransomware-related data theft and the growing risk of sensitive information being exposed through AI tools and applications.

85% of BEC incidents originated from phishing

An 11% increase year-over-year as threat actors leverage AI to create more convincing and effective attacks.

77% of organisations using negotiation services did not pay a ransom

An 11% increase year-over-year as threat actors leverage AI to create more convincing and effective attacks.

The report also highlights how organisations with strong security fundamentals are better positioned to prevent, detect and respond to evolving threats.

Strong security starts with strong foundations.

The Arctic Wolf 2026 Threat Report found that organisations investing in identity, segmentation, logging, secure remote access and continuous monitoring were better positioned to defend against today's most common threats.

You don't need perfect security.
You need security built for how attacks really unfold.



Ismael Valenzuela

Vice President of Labs,
Threat Research & Intelligence
at Arctic Wolf



Read the full
2026 Threat Report

arcticwolf.com/resources/report



THE FORTEM TECHNOLOGY FRAMEWORK

Technology you can trust.

One strategic partner. Six connected customer outcomes.

Fortem connects business priorities to the right technology, services and partner capabilities—creating a clear route from challenge to outcome.

OUTCOMES ACROSS THE IT LIFECYCLE



FORTIFY

Protect what matters.

Reduce risk, strengthen security posture and support compliance.
IDENTITY & ACCESS · ENDPOINT · NETWORK · EMAIL · CLOUD SECURITY



OPTIMISE

Maximise value.

Remove inefficiency and improve return from existing technology.
LICENSING · CLOUD COST · ASSET MANAGEMENT · CONSOLIDATION



RESILIENCE

Stay operational.

Protect critical operations and recover quickly from disruption.
BACKUP · DISASTER RECOVERY · CONTINUITY · CYBER RECOVERY



TRANSFORM

Drive innovation.

Accelerate modernisation and build a foundation ready for change.
CLOUD MIGRATION · INFRASTRUCTURE · AI · APPLICATIONS



ENABLE

Empower people.

Create a productive, connected workforce built around experience.
MODERN WORKPLACE · COLLABORATION · ENDPOINTS · ADOPTION



MANAGE

Deliver continuous improvement.

Coordinate technology activity through the right partner model.
LIFECYCLE · ADVISORY · PROCUREMENT · LICENSING · DEPLOYMENT

**Start with the outcome.
Build a clearer technology roadmap.**

Vendor-agnostic advice. Relevant partner capability. Clear next steps.

CONTACT FORTEM

hello@fortem-it.com · www.fortem-it.com
Sales +44 (0) 203 80 22 000
Admin +44 (0) 203 80 22 101

GLOBAL HQ — LONDON

Belmont, Belmont Road, Uxbridge, UB8 1HE

2026 WORK TREND INDEX ANNUAL REPORT

Agents, human agency,
and the opportunity for
every organisation

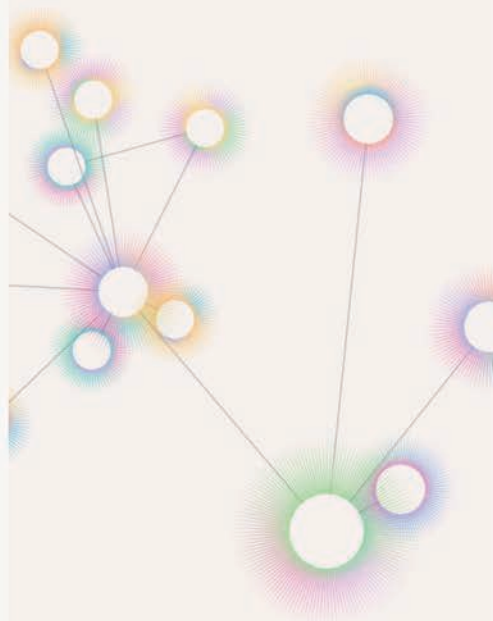
May 2026

**As AI and agents take on execution,
our own agency expands. The
question is whether organisations
are built to capture it.**

ORGANISATIONS

Every firm is a Learning System

The firms pulling ahead are focused on AI absorption rather than just AI adoption, redesigning how work gets done and turning output into insight. When that insight gets captured, shared, and built into how the organisation operates, it creates a self-reinforcing Learning System. Many leaders focus on hiring the right people and assume results will follow. But our data shows that it's something else: the conditions leaders create for that talent to thrive.



EMPLOYEES

AI lifts the ceiling on individual potential

AI is expanding what we can do— and putting a premium on judgement, clarity of intent, and the design of work itself. A privacy-preserving analysis of more than 100,000 chats in Microsoft 365 Copilot shows that 49% of all conversations support cognitive work—helping workers analyse information, solve problems, evaluate, and think creatively. The remainder splits among working with people (19%), finding information (15%), and producing work (17%). Employees at every level now have a partner that helps them analyse, synthesise, and deepen their own expertise, while also building expertise in other areas. AI is not just helping us do things faster. It's expanding who can do high-value work.

LEADERS

The job of every leader is to rearchitect work

Most organisations are not yet built to capture the value of this expanded human agency. The challenge is not isolated to tools or individuals—it's a breakdown across the system that connects leadership, culture, management practices, and how work is measured. To understand where this breakdown occurs, we mapped survey respondents across two dimensions: their capability with AI and their organisation's readiness to absorb it. Individual capability reflects how broadly respondents report using AI and how confidently they direct it, judge its output, and learn from it. It also includes how actively they experiment and share learnings, and whether they report creating new value with AI—from improving work quality and processes to enabling work they couldn't do before.



LOOKING AHEAD

The firms that build a new operating model today won't just move faster in the short term. They'll build something more durable, setting themselves up to create value in ways that we can't yet conceive of: an organisation that learns faster than its competitors, compounds its own intelligence, and gets harder to catch with every cycle.

This shift won't happen easily. Some jobs will change. Some will go away. And many that don't exist yet will emerge. According to LinkedIn's 2026 Labor Market Report, in the past two years, employers have created at least 1.3 million AI-related job opportunities, which include data annotators, AI engineers, and forward-deployed engineers. These roles didn't exist five years ago, but they have quickly become essential to digital economies. This kind of dynamism isn't new to work, but the pace and scale of it are—and the uncertainty people feel is real.

What's also real: The potential for employees to make impact has never been higher. Leaders are starting to redesign the systems around them. The organisations capturing what their work is teaching them are learning faster than the ones that aren't. None of that happens by accident.

The opportunity in front of every leader and organisation is to take control: to build a place where agents amplify what people can do, where human judgment stays at the centre of the work that matters, and where we all have the agency to decide what comes next. This is what AI can mean for all of us—if we choose to do the work to get there.

Get detailed executive guidance on how to build a Frontier Firm operating model across employees, leadership, and the organisation.

[MICROSOFT.COM/WORKLAB/WORK-TREND-INDEX](https://microsoft.com/worklab/work-trend-index)

Ready to turn AI potential into business value?

Fortem IT works with organisations to unlock the full value of Microsoft technologies, from AI and Copilot through to Azure, Security and Modern Work.

Come and chat to us on the Microsoft stand or contact sales@fortem-it.com after the event to find out how we can support your digital transformation journey.



AppCheck is a leading provider of continuous security testing, helping organisations identify and remediate vulnerabilities before attackers can exploit them. Our award-winning platform provides comprehensive visibility across complex web applications, APIs, cloud environments, infrastructure, and third-party supply chains, enabling organisations to discover, prioritise, and remediate vulnerabilities before they can be exploited.

Trusted by organisations across both the public and private sectors, AppCheck delivers actionable security insights that help security teams reduce risk, strengthen cyber resilience, and support compliance requirements through continuous vulnerability management.

EXCLUSIVE CYBERFEST OFFER

Claim a FREE Web Application Security Test

Gain valuable insight into the security of your public-facing web applications with a complimentary AppCheck Web Application Security Test.

To claim your free assessment, email
Emma.Lord@appcheck-ng.com
with the subject line:
CyberFest Free Trial

Our team will contact you to arrange your assessment and help you identify potential vulnerabilities affecting your application

Gigamon® protects the hybrid cloud networks and data of the world's most complex organisations. The AI-powered Gigamon Deep Observability Pipeline delivers complete visibility into all data in motion by providing trusted, network-derived telemetry directly to cloud, security, and observability tools. With AI-driven insights across packets, flows, and application metadata, organisations can detect threats concealed in encrypted and lateral traffic, resolve network and application performance bottlenecks, and validate compliance while reducing cost and complexity. Gigamon is trusted by over 4,000 organisations worldwide, including 83 of the Fortune 100, major mobile network operators, and public sector agencies at every level.

Gigamon's key products and services centre on the Deep Observability Pipeline, which delivers network-derived telemetry to cloud, security, observability, analytics, and AI tools. Core offerings include GigaVUE Cloud Suite for cloud visibility, GigaVUE appliances and network taps for data centre visibility, GigaSMART for traffic intelligence, and GigaVUE-FM for centralised orchestration and management.

Gigamon also provides application metadata intelligence, TLS/SSL decryption, and AI-powered capabilities.

LEARN MORE AT [GIGAMON.COM](https://www.gigamon.com)

Cambium Networks delivers intelligent networking solutions that help organisations build, manage, and secure reliable, high-performance networks. Its comprehensive portfolio includes fixed wireless broadband, enterprise Wi-Fi, switching, network security, and centralised cloud-based management.

Through Cambium ONE Network, these technologies work together as a unified ecosystem, simplifying operations, improving visibility, and enabling customers to scale their infrastructure with confidence. At the heart of the portfolio, cnMaestro provides centralised monitoring, automation, and actionable insights through a single, intuitive interface.

Key services:

- Fixed wireless broadband
- Enterprise Wi-Fi
- Network switching
- Network security
- Centralised cloud-based network management through cnMaestro.

Visit cambiumnetworks.com or email carmen.palumbo@cambiumnetworks.com

AUTHENTREND

COMPANY PROFILE

AuthenTrend's mission is to make authentication simple and immediate for everyone.

From enterprise IT teams to the people they protect. We believe logging into your accounts should not be a burden. No passwords to forget. No PINs to expose. No tokens to manage. Just biometric authentication that is both effortless and unphishable.

As digital access expands across devices, apps and clouds, password fatigue and credential theft remain top enterprise threats. The next generation of security must be personal, frictionless and universally deployable.

**Learn more at authentrend.com
Contact us at hello@fortem-it.com**

Gloucestershire's hub for cyber security and technology, serving as the go-to destination for connecting diverse minds and enabling secure innovation and growth for professionals and businesses operating in these sectors.

CyNam is your Gloucestershire-focused cyber and tech network, welcoming SMEs, large organisations, investors, local and central government representatives, and everyone in between. With a wide variety of activities running through the year, CyNam has something for everyone. Engage with CyNam by attending events, signing up to receive regular updates and becoming part of one of our many programmes.

Our events and initiatives serve as platforms for collaboration, where expertise is shared, and novel ideas are brought to life.

CyNam is building a thriving entrepreneurial community where people come together from all backgrounds, to collaborate, innovate and develop secure technologies that tackle global challenges and fuel economic growth.

If you are interested in supporting Cheltenham and Gloucestershire's flourishing cyber and tech ecosystem, don't hesitate to contact us to explore sponsorship opportunities, too.

Contact us: info@cynam.org

Learn more and see our latest events: cynam.org



The Future of Cybersecurity is Agentic



AI-powered attackers are increasing pressure on already stretched IT and security teams, but operationalizing agentic AI remains one of the most difficult challenges in cybersecurity today. Many current approaches require organizations to upgrade infrastructure, build agents, validate outcomes, and absorb added cost and complexity before value is realized. Instead of accelerating results, they add cost, delay time to value, and push more operational burden onto security teams.

Why it Works

Agent-Led with Humans in the Loop

The Aurora Agentic SOC transforms the traditional human-led SOC with an agent-led operating model built to run at machine speed. Specialized agents work across core SOC functions in parallel, while human experts remain involved in critical decisions, escalation, and oversight.

Turnkey by Design

The Aurora Agentic SOC is delivered as a fully operational agentic security operations center in as little as ten days. All agents are built in and operational with no additional setup, integration work, or model management required, so organizations do not need to build data lakes, deploy agentic tools, or validate experimental AI systems to realize value.

Enhanced Concierge Experience

The Aurora Agentic SOC strengthens the Concierge Experience™ by creating more capacity for Arctic Wolf security teams to be proactive, applying customer-specific context in every workflow, and preserving direct access to named experts. As agents take on more routine work, customers continue working with their Concierge Security Team while benefiting from higher-quality outcomes, faster answers, and support shaped to their environment and priorities.

Meet the Agents

At the core of the Aurora Agentic SOC, the Swarm of Experts brings together Oversight Agents, Authoritative Agents, and Process Agents to coordinate, execute, and validate security operations work. The result is agent-led operations that are faster, more scalable, and more trustworthy.

Oversight Agents

Oversight Agents help coordinate the Swarm of Experts and review outcomes so work stays efficient, controlled, and aligned to defined standards.

- Swarm Orchestrator: Routes tasks across the Swarm and keeps investigations moving
- Swarm Judge: Validates outcomes and decisions to reinforce quality and trust

Authoritative Agents

Authoritative Agents are purpose-built domain experts for critical security functions. Their scope is intentionally bounded, helping ensure precise action, reliable outcomes, and escalation when additional judgment is needed.

Process Agents

Process Agents are hundreds of specialized agents that assist the Authoritative Agents with focused tasks across the entire SOC, including agentic SOAR.

You Can't Defend What You Can't See

Security built around detection assumes your visibility can be trusted. Attackers increasingly target that assumption itself, degrading, bypassing or manipulating the very tools defenders rely on to see them.

Bitdefender®

Most enterprise security programmes are built on a sound bet: collect rich telemetry, spot suspicious behaviour, respond fast. The blind spot is the sensor itself. If an attacker can weaken an endpoint agent, abuse a trusted process, manipulate identity context, or interfere with event collection, the defender's picture can turn partial at exactly the moment it matters most.

This isn't a theoretical concern. Driver abuse, telemetry tampering, identity manipulation, trusted process abuse and sensor deception are all variations on the same idea: visibility itself has become a target. Attackers don't need to outrun detection if they can quietly degrade or bypass it first. That's why resilience can't start only after an alert fire.

It has to begin earlier: reducing the opportunities an attacker has to act, preventing malicious execution, hardening the endpoint, and protecting the security stack from tampering before telemetry becomes the last line of defence. Detection still matters, but it works best as one layer in a system designed to keep functioning even when a single source of truth is challenged or deliberately falsified by attackers.

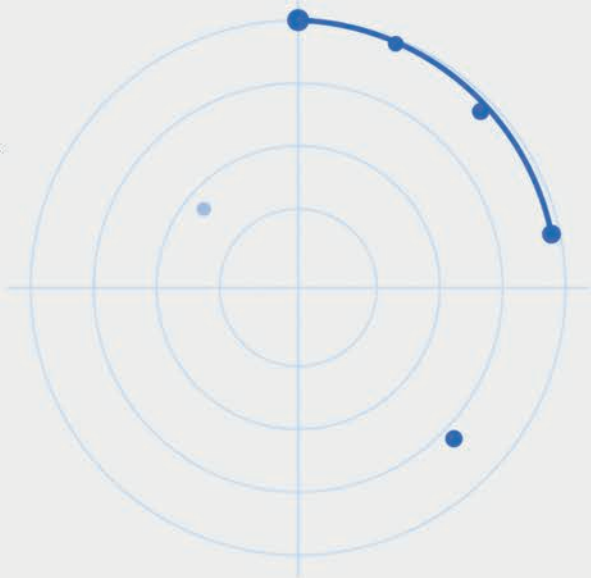
A more resilient model rests on three principles.

Prevent: block known and novel techniques before they execute. Constrain: reduce exposure, privilege and the paths available for lateral movement. Verify: correlate evidence continuously and test what you trust, rather than assuming a clean signal is a true one. In practice, this means closing routes attackers rely on before they're needed, through attack surface reduction, patch and configuration hardening, and least privilege design. It means layering exploit defence, fileless attack protection and tunable detection so no single control carries the full weight of the defence. And it means correlating evidence across endpoints, identities and applications, so analysts aren't reasoning from

one telemetry source that may itself be compromised.

Security leaders should ask a different question. Not "can we see the attack?" but "can we trust what we're seeing, and can our defences hold even when we can't?" Organisations that build for that assumption, rather than assuming visibility is guaranteed, are the ones best positioned when an attacker goes looking for the blind spot first.

Bitdefender.



Bitdefender®

COMPANY PROFILE

Security that sees further, and holds firm when it matters.

Bitdefender is a global cyber security leader, protecting over 500 million users across 170+ countries since 2001. Our GravityZone platform unifies prevention, protection, detection, and response, backed by an AI-driven threat intelligence engine built since 2008 that correlates evidence across endpoints, identities, networks and cloud, so defences hold even if one signal is compromised.

Alongside the platform, our Cyber Services team helps organisations pressure-test that resilience directly, from offensive testing to compliance support and incident readiness, so gaps get found before an attacker finds them.

Let's Build a Stronger Security Program – Together.

Learn more at bitdefender.com

OBJECT FIRST

Simply Resilient for Veeam

Secure, Simple and Powerful backup storage purpose-built for **Veeam** that enforces Zero Access, ensuring nobody can alter or delete backup data—even with admin credentials.

Absolute Immutability

Secure

- Zero Trust architecture with S3-native object storage
- Zero Access to perform destructive actions
- Third-party tested and verified

Simple

- No security expertise required
- 15 minutes to deploy and scale
- Updated and optimized automatically by Object First

Powerful

- Lightning-fast backups, up to 8 GB/s
- Supercharged Instant Recovery
- Capacity and performance scale linearly, supported by automatic load balancing

Ransomware-proof

When—not if—a breach occurs and your business, reputation, and career are on the line, backup storage with Absolute Immutability is your ultimate ransomware defence.



objectfirst.com





WHEN VISIBILITY FAILS, PROTECTION MUST NOT.

Go beyond detection with Bitdefender. Prevent attacks, protect security controls and strengthen resilience across your environment.

PREVENT

Reduce exposure and stop threats earlier.

PROTECT

Defend endpoints and the security stack.

RESPOND

Correlate evidence and act with confidence.

SEE MORE. TRUST MORE. STOP MORE.



cyberfest

2026



FORTEM
INFORMATION TECHNOLOGY



CYNAM



Microsoft

**IASME
CYBER
ASSURANCE**



**OBJECT
FIRST**

violet
+partners

AUTHENTREND



AppCheck

Lenovo

Acronis

FORTRA



Bitdefender

knowbe4